3GPP TSG-CN Meeting #26 **NP-040462**
8th – 10th December 2004. Athens, Greece.

3GPP TSG-CN1 Meeting #36 Tdoc N1-042078
Seoul, Korea, 15-19 November 2004

Title: **Reply LS on Security aspects of early IMS systems**
Response to: S3-040880 (N1-041673)
Release: Rel-6
Work Item: TEI6

Source: 3GPP TSG CN1
To: SA3, CN4, SA2
Cc: T2, CN

Contact Person:

Name: Peter Dawes

Tel. Number: +44 7717 275009

E-mail Address: peter.dawes@vodafone.com

Attachments: None

---

1. Overall Description:

CN1 thanks SA3 for their LS on Security aspects of early IMS systems. A related CR in N1-041846 was presented at CN1#36 proposing an Annex to TS 24.229 related to Security aspects of early IMS systems.

There was a concern that early IMS use, if specified in normative specifications would become a permanent one. In this respect TR would serve better.

It was agreed not to add the early IMS solution stage 3 as an annex to 24.229. CN1 does not make any recommendation on whether SA3 should take the proposed text and annex it to their early IMS TR 33.878.

The text presented in CN1#36, including the outcome of discussion, is included in this liaison.

2. Actions:

To 3GPP TSG CN

ACTION: CN1 asks TSG SA3 to take note of the text included in this liaison.

3. Date of Next TSG-CN1 Meetings:

CN1_37	14th – 18th February 2005	Sydney, Australia
CN1_38	25th – 30th April 2005	Cancun, Mexico

3 Definitions and abbreviations

3.1 Definitions

Early IMS UE: UE which implement the early IMS security solution specified in 3GPP TR 33.878 [19B]

Fully compliant UE: UEs which implement the security solution mechanisms specified in 3GPPTS 33.203 [19].

Annex D (Normative): Handling of Early IMS Security

D.1 Scope

This clause describes the security aspects during registration for the early IM CN subsystem as defined in TR 33.878 [19B].

The present annex defines specific requirements for an IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP) to allow for the security solution as described in 3GPP TR 33.878 [19B]. This security solution leads to different requirements with regards to Registration and Authentication.

D.2 Procedures at the UE

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include a Authorization header field and not include a Security-Client header field. The From header, To header, Contact header, Expires header, Request URI, Supported header and a P-Asserted-Id header shall be set according subclause 5.1.1.2.

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according subclause 5.1.1.2.

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

NOTE 2: The UE shall not use the temporary public user identity used for registration in any subsequent SIP requests.

D.3 Procedures at the P-CSCF

NOTE: As specified in RFC 3261[26], when the P-CSCF receives a SIP request from the early IMS UE, the P-CSCF checks the IP address in the “sent-by” parameter in the top of the Via header field. If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the P-CSCF adds a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received.

D.3.1 Registration

When the P-CSCF receives a REGISTER request from the UE that does not contain a Authorization header and not contain a Security-Client header, the P-CSCF shall handle the Path header, the Require header, the P-Charging-Vector header and the P-Visited-Network-ID header as described in subclause 5.2.12. Afterwards the P-CSCF shall determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) handle the Service-Route header, the public user identities, the P-Asserted-Identity header, the P-Charging-Function-Address header as described in subclause 5.2.2 for the reception of a 200 (OK) response; and

2) forward the 200 (OK) response to the UE.

D.3.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

As the security solution according 3GPP TR 33.878 [19B] does not offer IPSec, the P-CSCF shall implement the procedures as described in subclause 5.2.6 with the following deviations.

For requests initiated by the UE, when the P-CSCF receives a 1xx or 2xx response, the P-CSCF shall not rewrite its own Record Route entry.

For requests terminated by the UE, when the P-CSCF receives a request, prior to forwarding the request, the P-CSCF shall not include a protected server port in the Record-Route header and in the Via header.

D.4 Procedures at the I-CSCF

NOTE: Topology hiding is not available with early IMS security because topology hiding alters the "via" header.

D.5 Procedures at the S-CSCF

D.5.1 Registration

Upon receipt of an initial REGISTER request without an Authorization header, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) if no IP address is stored for the UE, query the HSS, as described in 3GPP TS 29.229 [15] with the public user ID as input and store the received IP address of the UE. Prior to contacting the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) check whether a "received" parameter exists in the top "via" header field. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the stored UE's IP address. If no "received" parameter exists in the top "via"" header field, then S-CSCF shall compare IP address received in the "sent-by" parameter against the stored UE IP address. In both cases, if the stored IP address and the IP address received in the top "via" header field do not match, the S-CSCF shall reject the registration with a 403 (Forbidden) response and skip the following steps.

5) handle the Cx Server Assignment procedure, the ICID, each non-barred registered public user identity, the Path header, the registration duration as described in subclause 5.4.1.2.2; and

6) send a 200 (OK) response to the UE as described in subclause 5.4.1.2.2.

D.5.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

On the reception of any request other than an initial REGISTER request, the S-CSCF shall check whether a "received" parameter exists in the top "via"" header field. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the UE's IP address stored during registration. If no "received" parameter exists in the top "via"" header field, then S-CSCF shall compare IP address received in the "sent-by" parameter against the IP address stored during registration. If the stored IP address and the IP address received in the top "via" header field do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response.

In case the stored IP address and the IP address receive in the top "via" header field do match, the S-CSCF shall proceed as described in 5.4.3.

D.6 Interworking between early IMS and fully compliant implementations during IMS registration

For interworking between early IMS and fully compliant implementations during IMS registration, the cases summarized following shall be supported.

Both UE and IMS network support early IMS only

IMS registration uses Early IMS security as described in this annex.

UE supports early IMS only, IMS network supports both early IMS and fully compliant access security

Early IMS security according to this annex shall be used for authenticating the UE for all registrations from UEs that do not provide the fully compliant security headers.

UE supports both, IMS network supports early IMS only

If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method shall be chosen. The UE shall use fully compliant security if the network supports this, otherwise the UE shall use early IMS security.

If the UE does not have such knowledge it shall start with the fully compliant registration procedure. The early IMS P-CSCF shall answer with a 420 "Bad Extension" failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message

NOTE: The Proxy-Require header cannot be ignored by the P-CSCF.

The UE shall, after receiving the error message, send an early IMS registration, i.e., shall send a new REGISTER request without the fully compliant security headers.

UE and IMS Network Support Both

The UE shall start with the fully compliant IMS registration procedure. The network, with receiving the initial REGISTER message, receives indication that the UE is fully compliant and shall continue as specified by TS 33.203[19].

UE and IMS network support both, UE contains a SIM

The UE might start with the fully compliant IMS registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error.

The S-CSCF shall answer with a 401 (Unauthorized) with an Error-info: header containing the text "Early security required". The UE then retries using early IMS security.

UE supports early IMS only, IMS network supports fully compliant access security only

The UE sends a REGISTER request to the IMS network that does not contain the security headers required by fully compliant IMS. The fully compliant P-CSCF will detect that the Security-Client header is missing and return a 4xx messages, as described in clause 5.2.2.

UE supports fully compliant access security only, IMS network supports early IMS only

The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 “Bad Extension” failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message. After receiving the error message, the UE shall stop the attempt to register with this network, since the fully 3GPP compliant security according to TS 33.203[19] is not supported.

Early IMS Authentication Fails

If early authentication fails, for example because the source address of IP packets does not match the IP address in the Via header when checked at the P-CSCF, the network returns 403 (Forbidden) to the UE.